Steiner quadruple systems $S(n, 4, 3)$ of a fixed corank

D.V. Zinoviev,, V.A. Zinoviev

A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

OC2013 Albena, Bulgaria, September 6-12, 2013

Outline

A Steiner Quadruple System $S(v, 4, 3)$ is a pair (X, B) where X is a set of v elements and B is a collection of 4-subsets (blocks) of X such that every 3-subset of X is contained in exactly one block of B.

A Steiner Quadruple System $S(v,4,3)$ is a pair (X,B) where X is a set of v elements and B is a collection of 4-subsets (blocks) of X such that every 3-subset of X is contained in exactly one block of B.
Hanani (1960) proved that a necessary condition for $S(v,4,3)$ $v \equiv 2$ or $4 \pmod 6$ is also sufficient. Enumeration problem of such non-isomorphic systems is solved only for $v \leq 16$:

Denote by $\gamma(v)$ the number of non-isomorphic such systems $S(v, 4, 3)$. The best known lower (Doyen-Vandensavel, 1971) and upper (Lenz, 1985) bounds are as follows:

Denote by $\gamma(v)$ the number of non-isomorphic such systems $S(v, 4, 3)$. The best known lower (Doyen-Vandensavel, 1971) and upper (Lenz, 1985) bounds are as follows:

$$(2)^{\frac{v^3}{24}} \leq \gamma(v) \leq (2)^{\frac{v^3}{24} \cdot \log v (1+o(1))} .$$

Denote by $\gamma(v)$ the number of non-isomorphic such systems $S(v,4,3)$. The best known lower (Doyen-Vandensavel, 1971) and upper (Lenz, 1985) bounds are as follows:

$$(2)^{\frac{v^3}{24}} \leq \gamma(v) \leq (2)^{\frac{v^3}{24}\cdot\log v(1+o(1))}.$$

Since $v! < 2^{v\cdot\log v}$ the number γ_v has the same coefficient near $v^3/24$ of the asymptotic expression (for growing v) as the number of different systems $S(v,4,3)$, which we denote by $\Gamma(v)$.

One of the parameter of an arbitrary $S_v = S(v,4,3)$ is its rank $\mathrm{rk}(S_v)$ - *the dimension of linear space over* $\mathbf{F}_2$*, generated by rows of the incidence matrix of* S_v.

One of the parameter of an arbitrary $S_v = S(v,4,3)$ is its rank $\mathrm{rk}(S_v)$ - *the dimension of linear space over* $\mathbf{F}_2$*, generated by rows of the incidence matrix of* S_v.
An arbitrary S_v of order $v = 2^m$ has a rank $\mathrm{rk}(S_v)$ over $\mathbf{F}_2$ (i.e. 2-rank) in the range:

$$2^m - m - 1 \leq \mathrm{rk}(S_v) \leq 2^m - 1.$$

One of the parameter of an arbitrary $S_v = S(v,4,3)$ is its rank $\mathrm{rk}(S_v)$ - *the dimension of linear space over* $\mathbf{F}_2$*, generated by rows of the incidence matrix of* S_v.
An arbitrary S_v of order $v = 2^m$ has a rank $\mathrm{rk}(S_v)$ over $\mathbf{F}_2$ (i.e. 2-rank) in the range:

$$2^m - m - 1 \leq \mathrm{rk}(S_v) \leq 2^m - 1.$$

Denote by $\Gamma(v,s)$ the number of different Steiner systems $S_v = S(v,4,3)$ with rank $\mathrm{rk}(S_v) \leq 2^m - m - 1 + s$.

A Steiner system $S(2^m, 4, 3)$ of the minimal rank, equal to $2^m - m - 1$, is called a Boolean system (its incident matrix is formed by the codewords of weight 4 of the binary extended Hamming code of length 2^m.

A Steiner system $S(2^m, 4, 3)$ of the minimal rank, equal to $2^m - m - 1$, is called a Boolean system (its incident matrix is formed by the codewords of weight 4 of the binary extended Hamming code of length 2^m.

Since the automorphism group of a Boolean system is the general linear group $GL(m, 2)$, there are

$$\Gamma(v, 0) = \frac{v!}{|GL(m, 2)|} =$$

$$= \frac{v!}{v(v-1)(v-2)(v-4)\cdots v/2}$$

different such Boolean systems of order $v = 2^m$.

Tonchev (2003) enumerated all different Steiner quadruple systems $S(2^m, 4, 3)$ of rank equal to $2^m - m$ (i.e. $s = 1$).

Tonchev (2003) enumerated all different Steiner quadruple systems $S(2^m, 4, 3)$ of rank equal to $2^m - m$ (i.e. $s = 1$).
In 2007 the authors enumerated all different Steiner systems SQS(2^m) of rank $\mathrm{rk}(S_v) \leq 2^m - m + 1$ (i.e. $s = 2$).

Tonchev (2003) enumerated all different Steiner quadruple systems $S(2^m,4,3)$ of rank equal to $2^m - m$ (i.e. $s = 1$).
In 2007 the authors enumerated all different Steiner systems SQS(2^m) of rank $\mathrm{rk}(S_v) \leq 2^m - m + 1$ (i.e. $s = 2$).
The goal of the present work is to enumerate all different Steiner systems $S(2^m,4,3)$ of the 2-rank not greater than $2^m - m - 1 + s$, where $0 \leq s \leq m - 1$.

Denote by K a q-ary MDS $(4, 2, q^3)_q$-code over the alphabet $\{0, 1, \dots, q-1\}$ and by $\Gamma_K(q)$ denote the number of different such codes K.

Denote by K a q-ary MDS $(4, 2, q^3)_q$-code over the alphabet $\{0, 1, \ldots, q-1\}$ and by $\Gamma_K(q)$ denote the number of different such codes K.

Lemma 1.

(Potapov-Krotov-Sokolova, 2008). If $q = 2^s$, then

$$\Gamma_K(q) \geq 2^{(q/2)^3}.$$

Suppose $u = 2^{m-s}$ and $q = 2^s$. Let $X_u = \{1, \ldots, u\}$,
$X_q(j) = \{q(j-1)+1, \ldots, qj\}$

Suppose $u = 2^{m-s}$ and $q = 2^s$. Let $X_u = \{1,\dots,u\}$,
$X_q(j) = \{q(j-1)+1,\dots,qj\}$
Given:

- an arbitrary $S(u,4,3)$, the set of elements X_u;

Suppose $u = 2^{m-s}$ and $q = 2^s$. Let $X_u = \{1, \ldots, u\}$,
$X_q(j) = \{q(j-1)+1, \ldots, qj\}$
Given:

- an arbitrary $S(u, 4, 3)$, the set of elements X_u;
- arbitrary $h = u(u-1)(u-2)/24$ codes $K_1, \ldots, K_h$;

Suppose $u = 2^{m-s}$ and $q = 2^s$. Let $X_u = \{1, \ldots, u\}$,
$X_q(j) = \{q(j-1)+1, \ldots, qj\}$
Given:

- an arbitrary $S(u, 4, 3)$, the set of elements X_u;
- arbitrary $h = u(u-1)(u-2)/24$ codes $K_1, \ldots, K_h$;
- arbitrary $u(u-1)/2$ systems $S(2q, 4, 3)$ not of the full rank, enumerated $S_{2q}(j_1, j_2)$, where $1 \le j_1 < j_2 \le u$, the set of elements $X_q(j_1) \bigcup X_q(j_2)$;

Suppose $u = 2^{m-s}$ and $q = 2^s$. Let $X_u = \{1, \ldots, u\}$,
$X_q(j) = \{q(j-1)+1, \ldots, qj\}$
Given:

- an arbitrary $S(u, 4, 3)$, the set of elements X_u;
- arbitrary $h = u(u-1)(u-2)/24$ codes $K_1, \ldots, K_h$;
- arbitrary $u(u-1)/2$ systems $S(2q, 4, 3)$ not of the full rank, enumerated $S_{2q}(j_1, j_2)$, where $1 \leq j_1 < j_2 \leq u$, the set of elements $X_q(j_1) \bigcup X_q(j_2)$;
- arbitrary u systems $S(q, 4, 3)$, enumerated $S_q(j)$, $\quad j = 1, \ldots, u$, with the set of elements $X_q(j)$.

Define three sets: $S^{(1,1,1,1)}$,$S^{(2,2)}$,$S^{(4)}$ of blocks of size 4, of elements

$$X_{uq} = \bigcup_{j=1}^{u} X_q(j) = \{1, 2, \ldots, uq\}.$$

Construction II(s)

The set $S^{(1,1,1,1)}$ is a union of 4-sets $C(\boldsymbol{c}_i; K_i)$:

$$S^{(1,1,1,1)} = \bigcup_{i=1}^{h} C(\boldsymbol{c}_i; K_i)$$

where $h = u(u-1)(u-2)/24$, $\boldsymbol{c}_i \in S(u,4,3)$ and

$$C(\boldsymbol{c}_i; K_i) = \{(qi_1 + a_1, qi_2 + a_2, qi_3 + a_3, qi_4 + a_4) : \ (a_1, a_2, a_3, a_4) \in K_i\}$$

where $\boldsymbol{c}_i = (i_1 + 1, i_2 + 1, i_3 + 1, i_4 + 1)$.

The set $S^{(2,2)}$ is a union of $u(u-1)/2$ sets $W(j_1, j_2)$:

$$S^{(2,2)} = \bigcup_{1 \le j_1 < j_2 \le u} W(j_1, j_2)$$

where

$$W(j_1, j_2) = S_{2q}(j_1, j_2) \setminus \left(S_q^{(\ell)}(j_1, j_2) \cup S_q^{(r)}(j_1, j_2) \right),$$

where $S_q^{(\ell)}(j_1, j_2)$ and $S_q^{(r)}(j_1, j_2)$ are two subsystems of $S_{2q}(j_1, j_2)$ with sets of elements $X_q(j_1)$ and $X_q(j_2)$;

The set $S^{(4)}$ is a union of u systems $S_q(j)$, where $S_q(j)$ has the element set $X_q(j)$:

$$S^{(4)} = \bigcup_{j=1}^{u} S_q(j)$$

Main Results

Theorem 1. *The set*

$$S = S^{(1,1,1,1)} \bigcup S^{(2,2)} \bigcup S^{(4)}$$

is a Steiner system $S(v,4,3)$, $v = uq$, for any choice of the initial systems and codes.

Theorem 2. *Let $S_v = S(v,4,3)$ be a Steiner system of order $v = 2^m$ and of rank*

$$\mathrm{rk}(S_v) \leq 2^m - m - 1 + s.$$

Then the system S_v is obtained from a Boolean Steiner system $S_u = S(u,4,3)$ of order $u = 2^{m-s}$, using construction $II(s)$, described above, where $q = 2^s$.

Theorem 3. *The number* $\Gamma(v,s)$ *of different Steiner systems* $S_v = S(v,4,3)$ *of order* $v = 2^m$ *of rank not greater than* $v-1-m+s$, *whose incident matrices are all orthogonal to fixed* $[v, m+1-s, v/2]$*-code, satisfies the following equality:*

$$\Gamma(v,s) = (\Gamma_K)^{u(u-1)(u-2)/24} \times \left(\frac{\Gamma(2q,s+1)}{(\Gamma(q,s+1))^2}\right)^{u(u-1)/2} \times (\Gamma(q,s+1))^u ,$$

where $v = u \cdot q$ *and* $q = 2^s$*.*

Theorem 3. *The number $\Gamma(v,s)$ of different Steiner systems $S_v = S(v,4,3)$ of order $v = 2^m$ of rank not greater than $v-1-m+s$, whose incident matrices are all orthogonal to fixed $[v, m+1-s, v/2]$-code, satisfies the following equality:*

$$\Gamma(v,s) = (\Gamma_K)^{u(u-1)(u-2)/24} \times \left(\frac{\Gamma(2q,s+1)}{(\Gamma(q,s+1))^2}\right)^{u(u-1)/2} \times (\Gamma(q,s+1))^u,$$

where $v = u \cdot q$ and $q = 2^s$.

Asymptotically when q is fixed and $u \to \infty$ we obtain that

$$\Gamma(v,s) > (2)^{c \cdot \frac{v^3}{24}}$$

where $c \to 1/8$.